Claims

What is claimed is:

1. A method for controlling access to one or more information items purchasable from a merchant and accessible over a network, wherein a user interested in a given information item is permitted to access a corresponding signed ciphertext of the given information item, the signed ciphertext having at least a first ciphertext portion, the method comprising the steps of:

receiving from the user a blinded version of the first ciphertext portion of the signed ciphertext in conjunction with a request from the user for purchase of the given information item from the merchant; and

decrypting the blinded version of the first ciphertext portion and returning to the user the resulting decrypted blinded version of the first ciphertext portion, wherein the resulting decrypted blinded version provides information that is utilized by the user in conjunction with accessing the given information item in a manner such that the merchant is unable to identify the given information item purchased by the user.

2. The method of claim 1 wherein the signed ciphertext for the given information item comprises the first ciphertext portion, a second ciphertext portion, an unencrypted description of the information item, and a tag, with at least a portion of the tag comprising a signature.

3. The method of claim 2 wherein the signature utilizes at least a part of the first ciphertext portion as a public key.

4. The method of claim 1 wherein the first ciphertext portion comprises a symmetric key encrypted using a public key associated with the merchant.

5. The method of claim 1 wherein the first ciphertext portion is encrypted using an ElGamal encryption technique.

6. The method of claim 1 wherein the signed ciphertext is signed using a Schnorr signature.

7. The method of claim 1 wherein the signed ciphertext further includes a second ciphertext portion corresponding to an encrypted version of the given information item.

8. The method of claim 1 wherein the user verifies a signature of the signed ciphertext before requesting purchase of the given information item.

9. The method of claim 1 wherein the decrypting step is implemented in a payment server associated with the merchant.

10. The method of claim 1 wherein the decrypted blinded version of the first ciphertext portion returned to the user further comprises a proof of correct decryption that allows the user to check that the decrypted blinded version for correctness.

11. The method of claim 1 wherein the decrypted blinded version of the first ciphertext portion returned to the user comprises a blinded key that when unblinded by the user is used to decrypt a second ciphertext portion of the signed ciphertext so as to obtain the purchased information item.

12. The method of claim 1 wherein the decrypting step is implemented in at least part of a set of multiple rounds, with the user providing a blinded ciphertext and receiving a corresponding decryption result for each of the rounds.

13. The method of claim 12 wherein the decrypting step is implemented in j rounds, and wherein for each of the first j-1 of the rounds the user provides a blinded ciphertext and receives in response a corresponding decryption result that is subsequently reblinded by the user and provided as the blinded ciphertext for the next round, and wherein a plaintext generated after the jth round provides the information that is utilized by the user in conjunction with accessing the given information item.

14. The method of claim 12 wherein the decrypting step is implemented in part of a set of j rounds, and wherein for each of the first j-1 of the rounds the user provides a blinded ciphertext and receives in response a corresponding decryption result, and wherein a plaintext generated after one of the first j-1 rounds provides the information that is utilized by the user in conjunction with accessing the given information item.

15. The method of claim 1 wherein the merchant establishes different public keys for use with different ones of a plurality of information items purchasable from the merchant.

16. A processor-based system for controlling access to one or more information items purchasable from a merchant and accessible over a network, wherein a user interested in a given information item is permitted to access a signed ciphertext version of the given information item, the signed ciphertext version having at least a first ciphertext portion, and wherein the system is operative: (i) to receive from the user a blinded version of the first ciphertext portion of the signed ciphertext in conjunction with a request from the user for purchase of the given information item from the merchant; and (ii) to decrypt the blinded version of the first ciphertext portion and return to the user the resulting blinded version of the first ciphertext portion, wherein the resulting blinded version provides information that is utilized by the user in conjunction with accessing the given information item in a manner such that the merchant is unable to identify the given information item purchased by the user.

17. A machine-readable medium containing one or more software programs for controlling access to one or more information items purchasable from a merchant and accessible over a network, wherein a user interested in a given information item is permitted to access a corresponding signed ciphertext having at least a first ciphertext portion, and wherein the one or more programs when executed implement the steps of:

receiving from the user a blinded version of the first ciphertext portion of the signed ciphertext in conjunction with a request from the user for purchase of the given information item from the merchant; and

decrypting the blinded version of the first ciphertext portion and returning to the user the resulting blinded version of the first ciphertext portion, wherein the resulting blinded version provides information that is utilized by the user in conjunction with accessing the given information item in a manner such that the merchant is unable to identify the given information item purchased by the user.

18. A method for controlling access to one or more information items purchasable from a merchant and accessible over a network, the method comprising the steps of:

receiving from the user a request for purchase of a given information item from the merchant, the request including information generated using at least a portion of an encrypted version of the given information item made accessible to the user without purchase of the given information item; and

returning to the user, in response to the request for purchase of the information item from the merchant, information that is utilized by the user to access the given information item in a manner such that the merchant is unable to identify the given information item purchased by the user.

19. A processor-based system for controlling access to one or more information items purchasable from a merchant and accessible over a network, wherein the system is operative: (i) to receive from the user a request for purchase of a given information item from the merchant, the request including information generated using at least a portion of an encrypted version of the given information item made accessible to the user without purchase of the given information item; and (ii) to return to the user, in response to the request for purchase of the information item from the merchant, information that is utilized by the user to access the given information item in a manner such that the merchant is unable to identify the given information item purchased by the user.

20. A machine-readable medium containing one or more software programs for controlling access to one or more information items purchasable from a merchant and accessible over a network, wherein the one or more programs when executed implement the steps of:

receiving from the user a request for purchase of a given information item from the merchant, the request including information generated using at least a portion of an encrypted version of the given information item made accessible to the user without purchase of the given information item; and

returning to the user, in response to the request for purchase of the information item from the merchant, information that is utilized by the user to access the given information item in a manner such that the merchant is unable to identify the given information item purchased by the user.